LEGAL // CASE STUDY

# Bolt Burdon + Trustd MTD

bolt burdon SOLICITORS

**SECTOR:**

Legal

**MOBILITY SETUP:**

COPE (iOS)

Meraki MDM

**DEVICES:**

iOS

**KEY RESULTS:**

An easy-to-deploy mobile security solution that protects staff from mobile phishing and cyberattacks over WiFi.

## A MOBILE SECURITY APP TO PROTECT CLIENT DATA

At Bolt Burdon they set the bar high. They are committed to exceptional service and don't settle for mediocre. Delivering nothing short of exceptional service, they demand the same from their suppliers.

To protect highly confidential data within the organisation, Bolt Burdon operates a COPE mobility strategy, providing managed iOS devices to their 80+ staff. They were looking for a comprehensive Mobile Threat Defence to layer powerful phishing and Man-in-the-Middle detection on top of their Mobile Device Management solution.

> *We have Trustd on every phone to protect against phishing and Man-in-the-Middle attacks, and we can see the health status of all our employees' devices. Trustd MTD gives us peace of mind that we're safeguarding the business data we access from our smartphones.*
>
> **GLEN SAMES,** IT Manager, Bolt Burdon

## MITIGATING RISK FROM MOBILE-BORNE THREATS

Bolt Burdon deployed Trustd MTD to all their corporate-owned iOS mobile devices through their MDM, Meraki. Thanks to Trustd's automatic enrollment API that works with all major MDM solutions, it future proofs their mobile solution stack - continuing to bolster their mobile security, while providing added Zero-Trust conditional access from mobile devices to their business data on Microsoft Cloud apps.

## PHISHING AND COMPROMISED WIFI

Protecting the confidentiality, integrity and availability of client information is paramount. The team at Bolt Burdon knows that providing work-only iOS devices is an important factor in limiting access to that data, but that added protection is needed against mobile phishing attacks designed to trick information out of users and Man-in-the-Middle attacks over public WiFi that can harvest credentials and other PII.

The Trustd app on every mobile device delivers lightweight, employee-privacy focused protection from these threats, while the administrative console provides visibility of device compliance status and real-time threats.

traced